Jun-12-23

# CYBER WEEKLY AWARENESS REPORT

JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "**HOW TO HACK FACEBOOK?**" ARE NOT ALLOWED
**FACEBOOK.COM/GROUPS/CYBERSECRETS**

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

LINUX

netSecurity®

# CYBER WEEKLY AWARENESS REPORT

## June 12, 2023

The Cyber WAR (Weekly Awareness Report) is an Open Source Intelligence AKA OSINT resource focusing on advanced persistent threats and other digital dangers received by over ten thousand individuals.  APTs fit into a cybercrime category directed at both business and political targets.  Attack vectors include system compromise, social engineering, and even traditional espionage.  Included are clickable links to news stories, vulnerabilities, exploits, & other industry risk.

## Summary

*Internet Storm Center Infocon Status*

INTERNET STORM CENTER infocon:GREEN http://isc.sans.edu

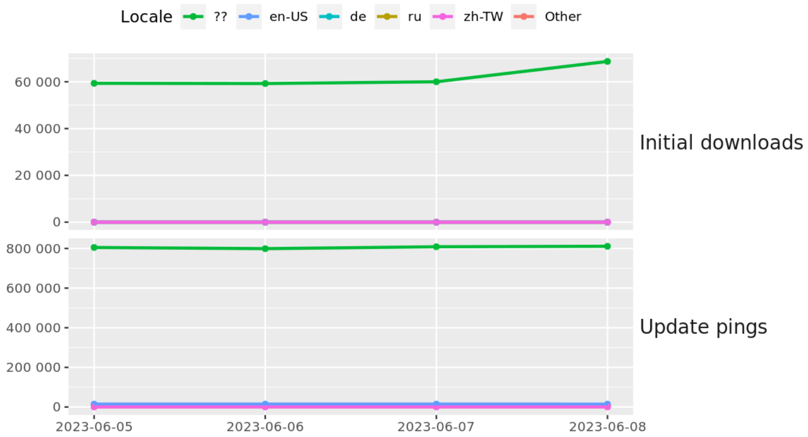
The intent of the 'Infocon' is to reflect changes in malicious traffic and the possibility of disrupted connectivity. In particular important is the concept of "Change". Every host connected to the Internet is subject to some amount of traffic caused by worms and viruses.

## Other IWC Publications

*Cyber Secrets books and ebook series can be found on Amazon.com at.* amzn.to/2UuIG9B

Cyber Secrets was originally a video series and is on both YouTube.

Tor Browser downloads and updates by locale



The Tor Project - https://metrics.torproject.org/

## Interesting News

* Free Cyberforensics Training - CSI Linux Basics

Download the distro and take the course to learn what CSI Linux can add to your arsenal.  This include a case management solution, document templates (reports and legal docs), and more GUI options for gathering digital evidence while storing it to the ongoing case.
https://training.csilinux.com/course/view.php?id=5

* * Our active Facebook group discusses the gambit of cyber security issues.  Join the Cyber Secrets Facebook group here.

# Index of Sections

Current News

* Packet Storm Security
* Krebs on Security
* Dark Reading
* The Hacker News
* Security Week
* Infosecurity Magazine
* KnowBe4 Security Awareness Training Blog
* ISC2.org Blog
* HackRead
* Koddos
* Naked Security
* Threat Post
* Null-Byte
* IBM Security Intelligence
* Threat Post
* C4ISRNET - Media for the Intelligence Age Military

The Hacker Corner:

* Security Conferences
* Google Zero Day Project

Cyber Range Content

* CTF Times Capture the Flag Event List
* Vulnhub

Tools & Techniques

* Packet Storm Security Latest Published Tools
* Kali Linux Tutorials
* GBHackers Analysis

InfoSec Media for the Week

* Black Hat Conference Videos
* Defcon Conference Videos
* Hak5 Videos
* Eli the Computer Guy Videos
* Security Now Videos
* Troy Hunt Weekly
* Intel Techniques: The Privacy, Security, & OSINT Show

Exploits and Proof of Concepts

* Packet Storm Security Latest Published Exploits
* CXSecurity Latest Published Exploits
* Exploit Database Releases

Cyber Crime & Malware Files/Links Latest Identified

* CyberCrime-Tracker

Advisories

* Hacked Websites
* Dark Web News
* US-Cert (Current Activity-Alerts-Bulletins)
* Zero Day Initiative Advisories
* Packet Storm Security's Latest List

Information Warfare Center Products

* CSI Linux
* Cyber Secrets Videos & Resoures
* Information Warfare Center Print & eBook Publications

# LATEST NEWS

## Packet Storm Security

* Online Muggers Make Serious Moves On Unpatched Microsoft Bugs
* Progress Software Issues New Critical Fix For MOVEit Transfer App
* Nvidia's AI Software Tricked Into Leaking Data
* FBI: FISA Section 702 Absolutely Critical To Spy On, Err, Protect Americans
* Ransomware Gang Clop Prepped Zero Day MOVEit Attacks In 2021
* Robinhood Markets Removes Three Crypto Tokens
* Netflix Sign-Ups Jump As Password Crackdown Kicks Off
* Google Changes Email Authentication After Spoof Shows A Bad Delivery For UPS
* Dozens Of Popular Minecraft Mods Found Infected With Fracturiser Malware
* VMware Discloses Trio Of High Severity Bugs In Network Monitoring Tool
* Hacker Attempts To Exploit Old And New Bugs Up 55%
* People Are Pirating GPT-4 By Scraping Exposed API Keys
* Deepfakes Of Victims Used In Sextortion Attacks Spike, FBI Warns
* BBC, BA, And Boots Issued With Ultimatum By Cyber Gang Clop
* What's Really Changed 10 Years After The Snowden Revelations
* ByteDance Accused Of Helping China Spy On Hong Kong Activists
* Crypto Catastrophe Stikes Some Atomic Wallet Users, Over $35 Million Thought Stolen
* Microsoft To Pay $20m For Child Privacy Violations
* MoveIt Hack: What Actions Can Data Breach Victims Take?
* SEC Accuses Coinbase Cryptocurrency Exchange Of Breaking US Regulations
* Ransomware Attacks Have Room To Grow, Verizon Report Shows
* U.S. Senate Leader Schedules Classified AI Briefings
* Qbot Malware Adapts To Live Another Day... And Another...
* Amazon's Ring Doorbell Was Used To Spy On Customers
* Millions Of Users Vulnerable To Zero Day In MOVEit File Transfer App

## Krebs on Security

* Barracuda Urges Replacing - Not Patching - Its Email Security Gateways
* Service Rents Email Addresses for Account Signups
* Ask Fitis, the Bear: Real Crooks Sign Their Malware
* Discord Admins Hacked by Malicious Bookmarks
* Phishing Domains Tanked After Meta Sued Freenom
* Interview With a Crypto Scam Investment Spammer
* Russian Hacker "Wazawaka" Indicted for Ransomware
* Re-Victimization from Police-Auctioned Cell Phones
* Microsoft Patch Tuesday, May 2023 Edition
* Feds Take Down 13 More DDoS-for-Hire Services

# LATEST NEWS

### Dark Reading

* RomCom Threat Actor Targets Ukrainian Politicians, US Healthcare
* 10 Important Security Tasks You Shouldn't Skip
* 'Stealth Soldier' Attacks Target Libyan Government Entities With Surveillance Malware
* Supply Chain Attack Defense Demands Mature Threat Hunting
* Doing Less With Less: Focusing on Value
* Passkeys See Fresh Momentum With New Pilot Programs
* DOS Attacks Dominate, but System Intrusions Cause Most Pain
* Brand-New Security Bugs Affect All MOVEit Transfer Versions
* 'Asylum Ambuscade' Cyberattackers Blend Financial Heists & Cyber Espionage
* 3 Elite Communication Skills to Help Security Pros Get Projects Funded
* Cl0P Gang Sat on Exploit for MOVEit Flaw for Nearly 2 Years
* South African Female Students Offered Cyber Scholarship
* 5 Tips for Modernizing Your Security Operations Center Strategy
* How Continuous Monitoring and Threat Intel Can Help Prevent Ransomware
* City of Dallas Still Clawing Back Weeks After Cyber Incident
* QuSecure Awarded US Army Contract for Post-Quantum Cybersecurity Solutions
* Cybercrooks Scrape OpenAI API Keys to Pirate GPT-4
* Cybersecurity Institute to Open in Saudi Arabia
* Barracuda Warns ESG Appliances Need Urgent Rip & Replace
* The Growing Cyber Threats of Generative AI: Who's Accountable?

### The Hacker News

* Researchers Uncover Publisher Spoofing Bug in Microsoft Visual Studio Installer
* Why Now? The Rise of Attack Surface Management
* Cybercriminals Using Powerful BatCloak Engine to Make Malware Fully Undetectable
* Password Reset Hack Exposed in Honda's E-Commerce Platform, Dealers Data at Risk
* Beware: 1,000+ Fake Cryptocurrency Sites Trap Users in Bogus Rewards Scheme
* Critical RCE Flaw Discovered in Fortinet FortiGate Firewalls - Patch Now!
* Apple's Safari Private Browsing Now Automatically Removes Tracking Parameters in URLs
* New SPECTRALVIPER Backdoor Targeting Vietnamese Public Companies
* New Critical MOVEit Transfer SQL Injection Vulnerabilities Discovered - Patch Now!
* Microsoft Uncovers Banking AitM Phishing and BEC Attacks Targeting Financial Giants
* Asylum Ambuscade: A Cybercrime Group with Espionage Ambitions
* 5 Reasons Why Access Management is the Key to Securing the Modern Workplace
* Stealth Soldier: A New Custom Backdoor Targets North Africa with Espionage Attacks
* Experts Unveil Exploit for Recent Windows Vulnerability Under Active Exploitation
* Clop Ransomware Gang Likely Aware of MOVEit Transfer Vulnerability Since 2021

# LATEST NEWS

### Security Week

* US Government Provides Guidance on Software Security Guarantee Requirements
* US Charges Russians With Hacking Cryptocurrency Exchange
* Intellihartx Informs 490k Patients of GoAnywhere-Related Data Breach
* Software Supply Chain: The Golden Container Ship
* New MOVEit Vulnerabilities Found as More Zero-Day Attack Victims Come Forward
* Swiss Fear Government Data Stolen in Cyberattack
* Fortinet Patches Critical FortiGate SSL VPN Vulnerability
* In Other News: AI Regulation, Layoffs, US Aerospace Attacks, Post-Quantum Encryption
* Blackpoint Raises $190 Million to Help MSPs Combat Cyber Threats
* Google Introduces SAIF, a Framework for Secure AI Development and Use

### Infosecurity Magazine

# LATEST NEWS

### KnowBe4 Security Awareness Training Blog RSS Feed

* Half of U.K. Companies Have Been a Cyber Attack Victim in the Last Three Years
* Forrester: AI, Cloud Computing, and Geopolitics are Emerging Cyberthreats in 2023
* Organizations Take 43 Hours to Detect an Spear Phishing Cyber Attack
* How NK's Cyber Criminals Stole 3 Billion in Crypto To Fund Their Nukes
* Verizon: Stolen Credentials Tops the List of Threat Actions in Breaches
* [SCAM OF THE WEEK] Summer Scams Your Users Should Watch Out For
* Why Companies Have Great Success Training Employees With Simulated Phishing Tests
* Verizon: Pretexting Now Tops Phishing in Social Engineering Attacks
* Verizon: 74% of Data Breaches Involve the "Human Element"
* Smishing Campaign Expands to the Middle East

### ISC2.org Blog

*Unfortunately, at the time of this report, the ISC2 Blog resource was not availible.*

### HackRead

* New Phishing Scam Spoofs German Media, Broadband Conference Anga
* Tracing the Path: Unraveling the Full History of Toncoin
* Minecraft Community on High Alert as Malware Infects Popular Mods
* 3rd-Party Reddit App Apollo Forced to Shut Down Due to API Charges
* IoT Botnet DDoS Attacks Threaten Global Telecom Networks, Nokia
* World Mobile's Africa Field Tests: Harnessing TV White Space and Starlink
* ChatGPT's False Information Generation Enables Code Malware

### Koddos

* New Phishing Scam Spoofs German Media, Broadband Conference Anga
* Tracing the Path: Unraveling the Full History of Toncoin
* Minecraft Community on High Alert as Malware Infects Popular Mods
* 3rd-Party Reddit App Apollo Forced to Shut Down Due to API Charges
* IoT Botnet DDoS Attacks Threaten Global Telecom Networks, Nokia
* World Mobile's Africa Field Tests: Harnessing TV White Space and Starlink
* ChatGPT's False Information Generation Enables Code Malware

# LATEST NEWS

### Naked Security

* History revisited: US DOJ unseals Mt. Gox cybercrime charges
* More MOVEit mitigations: new patches published for further protection
* Thoughts on scheduled password changes (don't call them rotations!)
* S3 Ep138: I like to MOVEit, MOVEit
* Firefox 114 is out: No 0-days, but one fascinating "teachable moment" bug
* Chrome and Edge zero-day: "This exploit is in the wild", so check your versions now
* MOVEit zero-day exploit used by data breach gangs: The how, the why, and what to do&hellip;
* Researchers claim Windows "backdoor" affects hundreds of Gigabyte motherboards
* S3 Ep137: 16th century crypto skullduggery
* Serious Security: That KeePass "master password crack", and what we can learn from it

### Threat Post

* Student Loan Breach Exposes 2.5M Records
* Watering Hole Attacks Push ScanBox Keylogger
* Tentacles of '0ktapus' Threat Group Victimize 130 Firms
* Ransomware Attacks are on the Rise
* Cybercriminals Are Selling Access to Chinese Surveillance Cameras
* Twitter Whistleblower Complaint: The TL;DR Version
* Firewall Bug Under Active Attack Triggers CISA Warning
* Fake Reservation Links Prey on Weary Travelers
* iPhone Users Urged to Update to Patch 2 Zero-Days
* Google Patches Chrome's Fifth Zero-Day of the Year

### Null-Byte

* These High-Quality Courses Are Only $49.99
* How to Perform Advanced Man-in-the-Middle Attacks with Xerosploit
* The Best-Selling VPN Is Now on Sale
* Unlock Facial Detection & Recognition on the Inexpensive ESP32-Based Wi-Fi Spy Camera
* Learn C# & Start Designing Games & Apps
* How to Set Up a Wi-Fi Spy Camera with an ESP32-CAM
* Get a Jump Start into Cybersecurity with This Bundle
* Hack Networks & Devices Right from Your Wrist with the Wi-Fi Deauther Watch
* This Top-Rated Course Will Make You a Linux Master
* Fingerprint Web Apps & Servers for Better Recon & More Successful Hacks

# LATEST NEWS

### IBM Security Intelligence

* Why Data Security is the Unsung Hero Driving Business Performance
* Merging DevOps and SecOps is a Great Idea: Get Started Now
* Security Awareness Training 101: Which Employees Need It?
* Beyond Requirements: Tapping the Business Potential of Data Governance and Security
* Secure-by-Design: Which Comes First, Code or Security?
* ITG10 Likely Targeting South Korean Entities of Interest to the Democratic People's Republic of Korea
* Will Commercial Spyware Survive Biden's Executive Order?
* SOCs Spend 32% of the Day On Incidents That Pose No Threat
* How to Boost Cybersecurity Through Better Communication
* Detecting Insider Threats: Leverage User Behavior Analytics

### InfoWorld

* Visual Studio 1.79 introduces read-only for files, folders
* How Grafana made observability accessible
* 6 finops best practices to reduce cloud costs
* Java 21 to drop generational Shenandoah GC
* When are containers or serverless a red flag?
* JetBrains adds to Aqua testing IDE
* Microsoft launches GPT-enabled Azure AI for US government agencies
* Composition vs. inheritance in OOP and C#
* 7 key features for Kubernetes and container security
* DataStax, Google partner to bring vector search to NoSQL AstraDB

### C4ISRNET - Media for the Intelligence Age Military

* Unmanned program could suffer if Congress blocks F-22 retirements, Hunter says
* UK to test Sierra Nevada's high-flying spy balloons
* Babcock inks deals to pitch Israeli tech for British radar, air defense programs
* This infantry squad vehicle is getting a laser to destroy drones
* As Ukraine highlights value of killer drones, Marine Corps wants more
* Army Space, Cyber and Special Operations commands form 'triad' to strike anywhere, anytime
* Shell companies purchase radioactive materials, prompting push for nuclear licensing reform
* Marine regiment shows off capabilities at RIMPAC ahead of fall experimentation blitz
* Maxar to aid L3Harris in tracking missiles from space
* US Army's 'Lethality Task Force' looks to save lives with AI

# The Hacker Corner

### Conferences

* 5 Things That Make The DEF CON Experience Special
* The 5 Most Controversial DEF CON Talks Of All Time
* 6 Notable DEF CON Moments
* Best AI Conferences To Attend in 2023
* How To Organize A Conference? Here's How To Get It Right!
* Virtual Conferences Marketing & Technology
* How To Plan an Event Marketing Strategy
* Zero Trust Cybersecurity Companies
* Types of Major Cybersecurity Threats In 2022
* The Five Biggest Trends In Cybersecurity  In 2022

### Google Zero Day Project

* Release of a Technical Report into Intel Trust Domain Extensions
* Multiple Internet to Baseband Remote Code Execution Vulnerabilities in Exynos Modems

### Capture the Flag (CTF)

**CTF Time** has links to a lot of current Capture the Flag competitions and information on past events.  Below is a list if CTFs they have on thier calendar.

* BSides Indore CTF 2023
* Codegate CTF 2023 Preliminary
* p4ctf 2023 finals
* Google Capture The Flag 2023
* AltayCTF 2023
* BSidesTLV 2023 CTF
* UIUCTF 2023
* Crypto CTF 2023
* Zh3r0 CTF v3 [POSTPONED]
* CyberSecurityRumble Quals

### VulnHub Downloadable CTFs for your Cyber Range (Most use VirtualBox)

* Matrix-Breakout: 2 Morpheus
* Web Machine: (N7)
* The Planets: Earth
* Jangow: 1.0.1
* Red: 1

# Tools & Techniques

### Packet Storm Security Tools Links

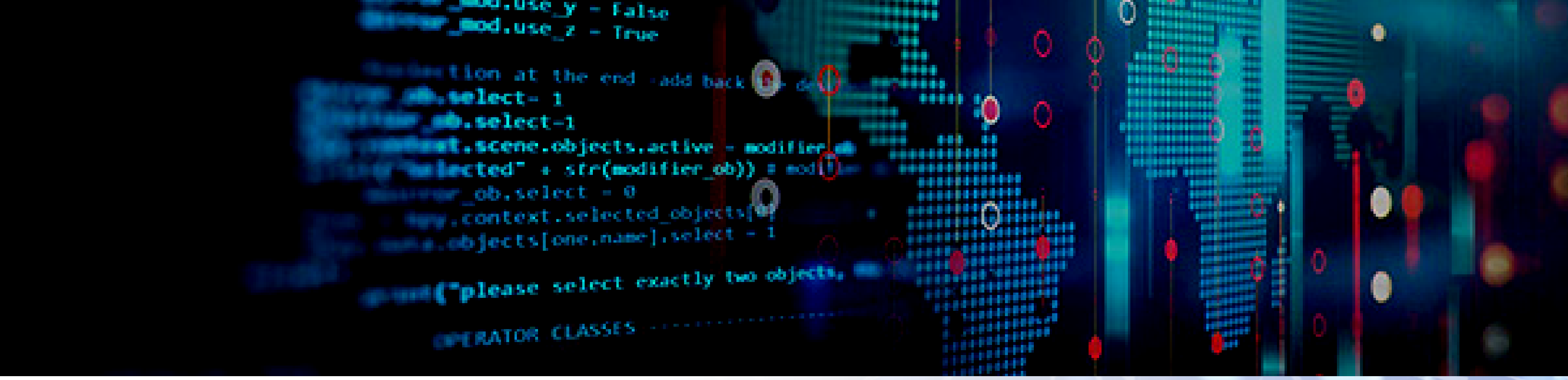
* Tenshi Log Monitoring Program 0.18
* Falco 0.35.0
* Faraday 4.4.0
* AIEngine 2.4.0
* OpenSSL Toolkit 3.1.1
* OpenSSL Toolkit 3.0.9
* OpenSSL Toolkit 1.1.1u
* Wireshark Analyzer 4.0.6
* tc Tor Chat Client
* Stegano 0.11.2

### Kali Linux Tutorials

* Mastering the Future: Key Data Science Skills for a Competitive Edge
* 5 Essential Crypto Tools For Linux Users In 2023
* QuadraInspect : Android Framework Providing A Powerful Tool For Analyzing The Security Of Android App
* Reportly : An AzureAD User Activity Report Tool
* From Endpoint Management to Experience Management - UEM Does It The Best!
* How to Use Ettercap to Intercept and Sniff Passwords
* WindowSpy : A Cobalt Strike Beacon Object File Meant For Targetted User Surveillance
* SilentMoonwalk - PoC Implementation Of A Fully Dynamic Call Stack Spoofer
* Unlock Your Employees' Potential: How UEM Can Help Achieve Employee Experience
* Taking Advantage of Emerging Betting Technologies

### GBHackers Analysis

* Microsoft Changed the Method of Naming the Hacker Groups
* Accidental 'write' Permissions In Alibaba PostgreSQL Let Attackers Access Sensitive Data
* Ex-Conti and FIN7 Hackers Team Up To Develop Domino Backdoor Malware
* ChatGPT Account Takeover Bug Allows Hackers To Gain User's Online Account
* Used Routers Fully Loaded With Corporate Secrets for Just $100



# Weekly Cyber Security Video and Podcasts

### SANS DFIR

* Protecting the Cloud from Ransomware | Host: Ryan Chapman | June 20, 2023
* What is the FOR528: Ransomware for Incident Responders course all about?
* SANS Threat Analysis Rundown | Katie Nickels
* SANS Threat Analysis Rundown | Katie Nickels

### Defcon Conference

* DEF CON 30 - Cesare Pizzi - Old Malware, New tools: Ghidra and Commodore 64
* DEF CON 30 BiC Village - Segun Olaniyan- Growth Systems for Cybersecurity Enthusiasts
* DEF CON 30 - Silk - DEF CON Memorial Interview
* DEF CON 30 Car Hacking Village - Evadsnibor - Getting Naughty on CAN bus with CHV Badge

### Hak5

* Amazon FINED For Privacy Violations - ThreatWire
* KeePass Master Passwords Could Be Stolen - ThreatWire
* Critical Flaw in Ruckus WiFi APs - Update Firmware ASAP - ThreatWire

### The PC Security Channel [TPSC]

* Edge vs Chrome: Phishing Test
* How to use Windows Firewall to block Hackers and Malware

### Eli the Computer Guy

* REDDIT GOES DARK - 6000 Subreddits go private over API fees
* MARK ZUCKERBERG DESTROYS APPLE VISON PRO - in his own mind
* TUCKER CARLSON "FAILS" on TWITTER - so sad...
* AI DEEPFAKE of TRUMP Kissing FAUCI???  DeSantis is Probably Legal

### Security Now

* Windows Platform Binary Table - OWASP, Tor anti-DoS protection, Mandatory SMB Signing on Win 11
* Brave's Brilliant Off the Record Request - .ZIP TLD, Bitwarden Passkey support, PyPi

### Troy Hunt

* Weekly Update 351

### Intel Techniques: The Privacy, Security, & OSINT Show

* 299-Self-Hosted 1: Introduction
* 298-OSINT Maintenance

# Proof of Concept (PoC) & Exploits

## Packet Storm Security

* Oracle Weblogic PreAuth Remote Command Execution
* TerraMaster TOS 4.2.15 Remote Code Execution
* TerraMaster TOS 4.2.06 Remote Code Execution
* Anevia Flamingo XL 3.2.9 Remote Root Jailbreak
* Anevia Flamingo XL 3.6.20 Authenticated Root Remote Code Execution
* Anevia Flamingo XS 3.6.5 Authenticated Root Remote Code Execution
* Anevia Flamingo XL/XS 3.6.x Default / Hardcoded Credentials
* OmniCart 3.4.0 Cross Site Scripting
* LearnDesk 1.0 Cross Site Scripting
* BB Machine Forum 1.0 Cross Site Scripting
* Expert X Jobs Portal And Resume Builder 1.0 Cross Site Scripting
* PhotoSwipe 5.3.7 Arbitrary File Download
* PES Pro CMS 1.9.7 Add Administrator
* KesionCMS X 9.5 Add Administrator
* Pannres-Idence CMS 7.3 Cross Site Request Forgery
* Ormesson-Immobilier CMS 8 SQL Injection
* osCommerce 4 Local File Inclusion
* WordPress Workreap 2.2.2 Shell Upload
* VIVO SPARQL Injection
* strongSwan VPN Charon Server Buffer Overflow
* librelp Remote Code Execution
* polkit File Descriptor Exhaustion
* Facebook Fizz Denial Of Service
* Ansible Fetch Path Traversal
* libssh2 1.8.2 Out-Of-Bounds Read

## CXSecurity

* Thruk Monitoring Web Interface 3.06 Path Traversal
* WordPress Theme Workreap 2.2.2 Unauthenticated Upload Leading to Remote Code Execution
* ManageEngine ADManager Plus Command Injection
* SCM Manager 1.60 Cross Site Scripting
* Screen SFT DAB 600/C Authentication Bypass Admin Password Change
* Laravel 10.11 Database Disclosure / Information Disclosure
* Screen SFT DAB 600/C Authentication Bypass Reset Board Config

# Proof of Concept (PoC) & Exploits

### Exploit Database

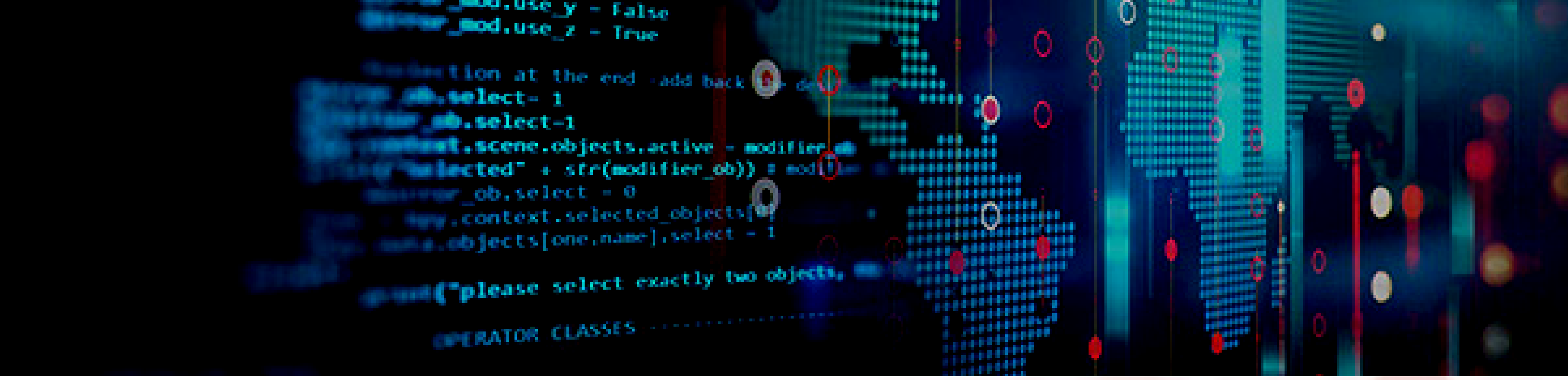
* [webapps] WordPress Theme Workreap 2.2.2 - Unauthenticated Upload Leading to Remote Code Execution
* [webapps] Thruk Monitoring Web Interface 3.06 - Path Traversal
* [local] USB Flash Drives Control 4.1.0.0 - Unquoted Service Path
* [webapps] Tree Page View Plugin 1.6.7 - Cross Site Scripting (XSS)
* [local] Macro Expert 4.9 - Unquoted Service Path
* [webapps] File Manager Advanced Shortcode 2.3.2 - Unauthenticated Remote Code Execution (RCE)
* [webapps] MotoCMS Version 3.4.3 - SQL Injection
* [webapps] STARFACE 7.3.0.10 - Authentication with Password Hash Possible
* [webapps] Barebones CMS v2.0.2 - Stored Cross-Site Scripting (XSS) (Authenticated)
* [webapps] Enrollment System Project v1.0 - SQL Injection Authentication Bypass (SQLI)
* [webapps] Total CMS 1.7.4 - Remote Code Execution (RCE)
* [webapps] MotoCMS Version 3.4.3 - Server-Side Template Injection (SSTI)
* [webapps] Pydio Cells 4.1.2 - Server-Side Request Forgery
* [webapps] Pydio Cells 4.1.2 - Cross-Site Scripting (XSS) via File Download
* [webapps] Pydio Cells 4.1.2 - Unauthorised Role Assignments
* [webapps] Faculty Evaluation System 1.0 - Unauthenticated File Upload
* [webapps] Online Security Guards Hiring System 1.0 - Reflected XSS
* [remote] Flexense HTTP Server 10.6.24 - Buffer Overflow (DoS) (Metasploit)
* [webapps] unilogies/bumsys v1.0.3 beta - Unrestricted File Upload
* [webapps] SCRMS 2023-05-27 1.0 - Multiple SQL Injection
* [webapps] Rukovoditel 3.3.1 - CSV injection
* [webapps] Camaleon CMS v2.7.0 - Server-Side Template Injection (SSTI)
* [webapps] SCM Manager 1.60 - Cross-Site Scripting Stored (Authenticated)
* [remote] Seagate Central Storage 2015.0916 - Unauthenticated Remote Command Execution (Metasploit)
* [webapps] Ulicms 2023.1 - create admin user via mass assignment

### Exploit Database for offline use

Kali has the Exploit-DB preinstalled and updates the database on a monthly basis. The tool that they have added is called "SearchSploit". This can be installed on Linux, Mac, and Windows. Using the tool is also quite simple. In the command line, type:

```
user@yourlinux:~$ searchsploit keyword1 keyword2
```

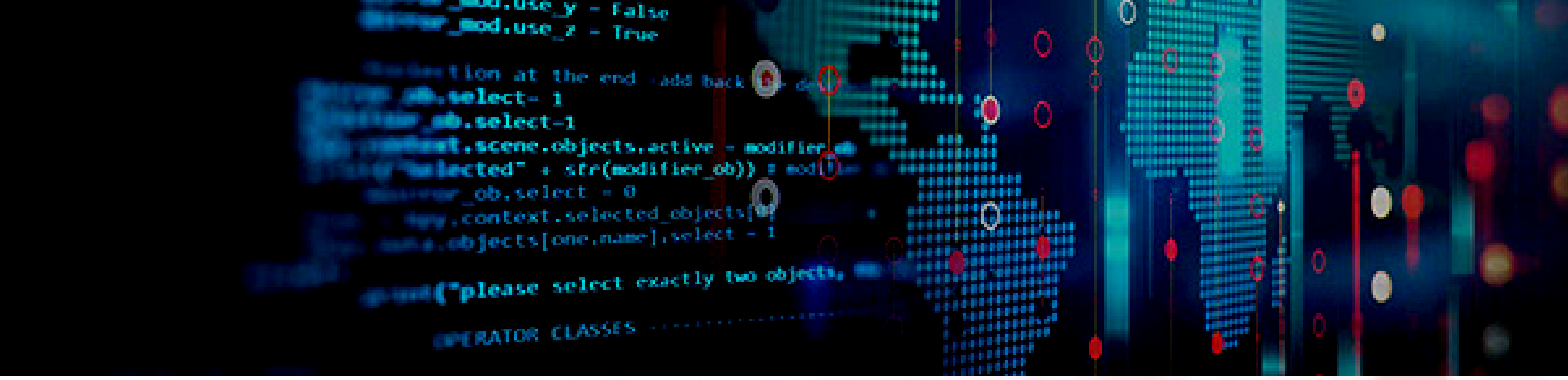
There is a second tool that uses searchsploit and a few other resources writen by 1N3 called "FindSploit". It is also a command line (CLI) tool used to search for exploits, but it also requires online access.


_mod.use_y = False
_mod.use_z = True
tion at the end -add back
ob.select= 1
ob.select=1
.scene.objects.active = modifier_ob
"selected" + str(modifier_ob)) # mod
_ob.select = 0
.context.selected_objects[
.objects[one.name].select = 1
("please select exactly two objects,
OPERATOR CLASSES

# Latest Hacked Websites

**Published on Zone-h.org**

https://dprd.kaltimprov.go.id/storage/net.html
https://dprd.kaltimprov.go.id/storage/net.html notified by Desktop77N3T
https://sidekstana.kaltaraprov.go.id/storage/net.html
https://sidekstana.kaltaraprov.go.id/storage/net.html notified by Desktop77N3T
https://tdp.p3.gov.np/V.txt
https://tdp.p3.gov.np/V.txt notified by EbRaHiM-VaKeR
https://www.revistageminis.ufscar.br/public/site/images/hacked/hackedbydr3v1l.gif
https://www.revistageminis.ufscar.br/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
http://ejournal-balitbang.kkp.go.id/public/site/images/hacked/hackedbydr3v1l.gif
http://ejournal-balitbang.kkp.go.id/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
http://revista.macn.gov.ar/ojs/public/site/images/hacked/hackedbydr3v1l.gif
http://revista.macn.gov.ar/ojs/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
https://cadernos.esp.ce.gov.br/public/site/images/hacked/hackedbydr3v1l.gif
https://cadernos.esp.ce.gov.br/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
http://jna.bio.gov.ua/public/site/images/hacked/hackedbydr3v1l.gif
http://jna.bio.gov.ua/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
http://mhn.bphn.go.id/public/site/images/hacked/hackedbydr3v1l.gif
http://mhn.bphn.go.id/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
https://anaismhn.museus.gov.br/public/site/images/hacked/hackedbydr3v1l.gif
https://anaismhn.museus.gov.br/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
https://journal.bappenas.go.id/public/site/images/hacked/hackedbydr3v1l.gif
https://journal.bappenas.go.id/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
http://borobudur.kemdikbud.go.id/public/site/images/hacked/hackedbydr3v1l.gif
http://borobudur.kemdikbud.go.id/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
https://ojs.wpro.who.int/ojs/public/site/images/hacked/hackedbydr3v1l.gif
https://ojs.wpro.who.int/ojs/public/site/images/hacked/hackedbydr3v1l.gif notified by Dr.3v1l
https://tlhp-new.sulselprov.go.id/a.txt
https://tlhp-new.sulselprov.go.id/a.txt notified by ./unn0rmaL
https://makaversenews.makassarkota.go.id/hacked.txt
https://makaversenews.makassarkota.go.id/hacked.txt notified by ./unn0rmaL
https://ki.sultengprov.go.id/nai.txt
https://ki.sultengprov.go.id/nai.txt notified by ./unn0rmaL
https://simandau.kaltaraprov.go.id/a.txt
https://simandau.kaltaraprov.go.id/a.txt notified by ./unn0rmaL

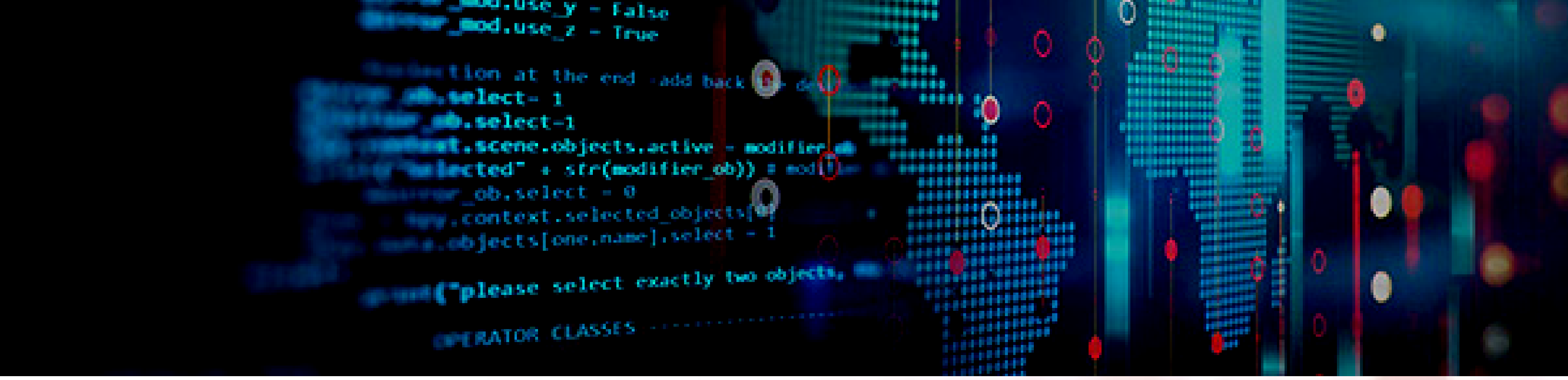


# Dark Web News

### Darknet Live

Opiates Vendor "DopeKingUSA"  Imprisoned for Distributing Fentanyl
One of the Operators of "CaliCartel" Drugs Vendor Account Sentenced
A Tennessee Woman Attempted to Hire a Hitman
Empire Market Drugs Vendor "Norco King" Imprisoned

### Dark Web Link



## Trend Micro Anti-Malware Blog

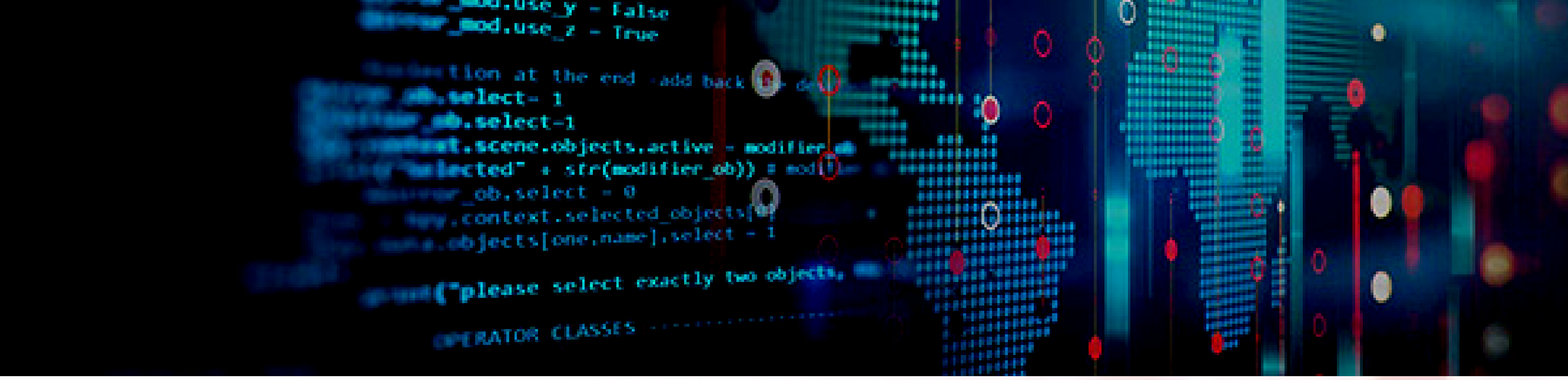
*Unfortunately, at the time of this report, the Trend Micro Anti-Malware Blog resource was not availible.*

## RiskIQ

* Skimming for Sale: Commodity Skimming and Magecart Trends in Q1 2022
* RiskIQ Threat Intelligence Roundup: Phishing, Botnets, and Hijacked Infrastructure 
* RiskIQ Threat Intelligence Roundup: Trickbot, Magecart, and More Fake Sites Targeting Ukraine 
* RiskIQ Threat Intelligence Roundup: Campaigns Targeting Ukraine and Global Malware Infrastructure
* RiskIQ Threat Intelligence Supercharges Microsoft Threat Detection and Response
* RiskIQ Intelligence Roundup: Spoofed Sites and Surprising Infrastructure Connections 
* RiskIQ Threat Intelligence Roundup: QBot, Magecart, Agent Tesla Headline Hijacked Infrastructure&nbsp
* RiskIQ Threat Intelligence Roundup: C2 and Nation-State Threat Infrastructure
* Jupyter Notebooks Make RiskIQ Data a Digital 'Mech Suit' for Threat Intelligence Analysts 
* "Offshore" Shinjiru Provides Bulletproof Services to Cyberattackers

## FireEye

* CVE-2023-27997: Critical Fortinet Fortigate Remote Code Execution Vulnerability
* Metasploit Weekly Wrap-Up
* OWASP TOP 10 API Security Risks: 2023!
* Detect and Prioritize Identity-Related Cloud Risk with InsightCloudSec
* CVE-2023-2868: Total Compromise of Physical Barracuda ESG Appliances
* Velociraptor 0.6.9 Release: Digging Even Deeper with SMB Support, Azure Storage and Lockdown Server M
* Metasploit Weekly Wrap-Up
* This is Ceti Alpha Five!
* Metasploit Weekly Wrap-Up
* Rapid7 Observed Exploitation of Critical MOVEit Transfer Vulnerability



# Advisories

### US-Cert Alerts & bulletins

* CISA Releases Two Industrial Control Systems Advisories
* VMware Releases Security Update for Aria Operations for Networks
* CISA Adds One Known Exploited Vulnerability to Catalog
* Mozilla Releases Security Updates for Multiple Products
* CISA and FBI Release #StopRansomware: CL0P Ransomware Gang Exploits MOVEit Vulnerability
* CISA Releases Two Industrial Control Systems Advisories
* CISA and Partners Release Joint Guide to Securing Remote Access Software
* CISA Adds Two Known Exploited Vulnerabilities to Catalog
* #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability
* People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection
* Vulnerability Summary for the Week of May 29, 2023
* Vulnerability Summary for the Week of May 22, 2023

### Zero Day Initiative Advisories

ZDI-CAN-20994: GStreamer
A CVSS score 8.8 (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'MICHAEL RANDRIANANTENAINA [https://elkamika.blogspot.com/]' was reported to the affected vendor on: 2023-06-12, 0 days ago. The vendor is given until 2023-10-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-20775: GStreamer
A CVSS score 7.6 (AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H) severity vulnerability discovered by 'Michael Randrianantenaina' was reported to the affected vendor on: 2023-06-12, 0 days ago. The vendor is given until 2023-10-10 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-21266: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-21032: Schneider Electric
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.
ZDI-CAN-21155: Siemens
A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to

publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21138: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21109: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21065: Schneider Electric

A CVSS score 7.8 (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21263: Siemens

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-09, 3 days ago. The vendor is given until 2023-10-07 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21252: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21371: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21387: Adobe

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Mat Powell of Trend Micro Zero Day Initiative' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21233: RARLAB

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'goodbyeselene' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21303: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21302: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21326: Foxit

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21035: Schneider Electric

A CVSS score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam)' was reported to the affected vendor on: 2023-06-08, 4 days ago. The vendor is given until 2023-10-06 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21236: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21224: Fuji Electric

A CVSS score 7.3 (AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Fritz Sands' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21292: Foxit

A CVSS score 3.3 (AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N) severity vulnerability discovered by 'Anonymous' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21238: Fuji Electric

A CVSS score 7.8 (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'kimiya' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-20731: Centreon

A CVSS score 7.5 (AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H) severity vulnerability discovered by 'Andreas Finstad' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21009: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

ZDI-CAN-21027: Microsoft

A CVSS score 8.8 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H) severity vulnerability discovered by 'Marcin Wiazowski' was reported to the affected vendor on: 2023-06-07, 5 days ago. The vendor is given until 2023-10-05 to publish a fix or workaround. Once the vendor has created and tested a patch we will coordinate the release of a public advisory.

## Packet Storm Security - Latest Advisories

Ubuntu Security Notice USN-6153-1

Ubuntu Security Notice 6153-1 - It was discovered that Jupyter Core executed untrusted files in the current working directory. An attacker could possibly use this issue to execute arbitrary code.

Red Hat Security Advisory 2023-3557-01

Red Hat Security Advisory 2023-3557-01 - OpenShift GitOps KAM OpenShift GitOps Kubernetes Application Manager CLI tool. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6152-1

Ubuntu Security Notice 6152-1 - It was discovered that NFS client's access cache implementation in the Linux kernel caused a severe NFS performance degradation in certain conditions. This updated makes the NFS file-access stale cache behavior to be optional.

Debian Security Advisory 5422-1

Debian Linux Security Advisory 5422-1 - It was discovered that jupyter-core, the core common functionality for Jupyter projects, could execute arbitrary code in the current working directory while loading configuration files.

Red Hat Security Advisory 2023-3555-01

Red Hat Security Advisory 2023-3555-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6151-1

Ubuntu Security Notice 6151-1 - It was discovered that the System V IPC implementation in the Linux kernel did not properly handle large shared memory counts. A local attacker could use this to cause a denial of service. It was discovered that the KVM VMX implementation in the Linux kernel did not properly handle indirect branch prediction isolation between L1 and L2 VMs. An attacker in a guest VM could use this to expose sensitive information from the host OS or other guest VMs.

Red Hat Security Advisory 2023-3556-01

Red Hat Security Advisory 2023-3556-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6150-1

Ubuntu Security Notice 6150-1 - Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-6149-1

Ubuntu Security Notice 6149-1 - Patryk Sondej and Piotr Krysiuk discovered that a race condition existed in the netfilter subsystem of the Linux kernel when processing batch requests, leading to a use-after-free vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code. Gwangun Jung discovered that the Quick Fair Queueing scheduler implementation in the Linux kernel contained an out-of-bounds write vulnerability. A local attacker could use this to cause a denial of service or possibly execute arbitrary code.

Ubuntu Security Notice USN-6147-1

Ubuntu Security Notice 6147-1 - Several security issues were discovered in the SpiderMonkey JavaScript library. If a user were tricked into opening malicious JavaScript applications or processing malformed data, a remote attacker could exploit a variety of issues related to JavaScript security, including denial of service attacks, and arbitrary code execution.

Debian Security Advisory 5421-1

Debian Linux Security Advisory 5421-1 - Multiple security issues have been found in the Mozilla Firefox web browser, which could potentially result in the execution of arbitrary code.

Ubuntu Security Notice USN-6146-1

Ubuntu Security Notice 6146-1 - It was discovered that Netatalk did not properly validate the length of user-supplied data in the DSI structures. A remote attacker could possibly use this issue to execute arbitrary code with the privileges of the user invoking the programs. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS. It was discovered that Netatalk did not properly validate the length of user-supplied data in the ad_addcomment function. A remote attacker could possibly use this issue to execute arbitrary code with root privileges. This issue only affected Ubuntu 20.04 LTS and Ubuntu 22.04 LTS.

Red Hat Security Advisory 2023-3550-01

Red Hat Security Advisory 2023-3550-01 - Python is an interpreted, interactive, object-oriented programming language, which includes modules, classes, exceptions, very high level dynamic data types and dynamic typing. Python supports interfaces to many system calls and libraries, as well as to various windowing systems. Issues addressed include a bypass vulnerability.

Ubuntu Security Notice USN-6145-1

Ubuntu Security Notice 6145-1 - It was discovered that Sysstat incorrectly handled certain arithmetic multiplications. An attacker could use this issue to cause Sysstat to crash, resulting in a denial of service, or possibly execute arbitrary code. This issue was only fixed for Ubuntu 16.04 LTS. It was discovered that Sysstat incorrectly handled certain arithmetic multiplications in 64-bit systems, as a result of an incomplete fix for CVE-2022-39377. An attacker could use this issue to cause Sysstat to crash, resulting in a denial of service, or possibly execute arbitrary code.

Red Hat Security Advisory 2023-3410-01

Red Hat Security Advisory 2023-3410-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.12.20.

Debian Security Advisory 5420-1

Debian Linux Security Advisory 5420-1 - Multiple security issues were discovered in Chromium, which could result in the execution of arbitrary code, denial of service or information disclosure.

Red Hat Security Advisory 2023-3409-01

Red Hat Security Advisory 2023-3409-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.12.20.

Red Hat Security Advisory 2023-3363-01

Red Hat Security Advisory 2023-3363-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the container images for Red Hat OpenShift Container Platform 4.10.61. Issues addressed include a denial of service vulnerability.

Ubuntu Security Notice USN-6144-1

Ubuntu Security Notice 6144-1 - It was discovered that LibreOffice did not properly validate the number of parameters passed to the formula interpreter, leading to an array index underflow attack. If a user were tricked into opening a specially crafted spreadsheet file, an attacker could possibly use this issue to execute arbitrary code. Amel Bouziane-Leblond discovered that LibreOffice did not prompt the user before loading the host document inside an IFrame. If a user were tricked into opening a specially crafted input file, an attacker could possibly use this issue to cause information disclosure or execute arbitrary code.

Ubuntu Security Notice USN-6143-1

Ubuntu Security Notice 6143-1 - Multiple security issues were discovered in Firefox. If a user were tricked into opening a specially crafted website, an attacker could potentially exploit these to cause a denial of service, obtain sensitive information across domains, or execute arbitrary code. Jun Kokatsu discovered that Firefox did not properly validate site-isolated process for a document loaded from a data: URL that was the result of a redirect, leading to an open redirect attack. An attacker could possibly use this issue to perform phishing attacks.

Debian Security Advisory 5419-1

Debian Linux Security Advisory 5419-1 - Two vulnerabilities were discovered in c-ares, an asynchronous name resolver library.

Red Hat Security Advisory 2023-3362-01

Red Hat Security Advisory 2023-3362-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.10.61. Issues addressed include a resource exhaustion vulnerability.

Red Hat Security Advisory 2023-3525-01

Red Hat Security Advisory 2023-3525-01 - Flask is a lightweight but extensible web development framework for Python based on the Werkzeug WSGI toolkit, and the Jinja 2 template engine.

Red Hat Security Advisory 2023-3366-01

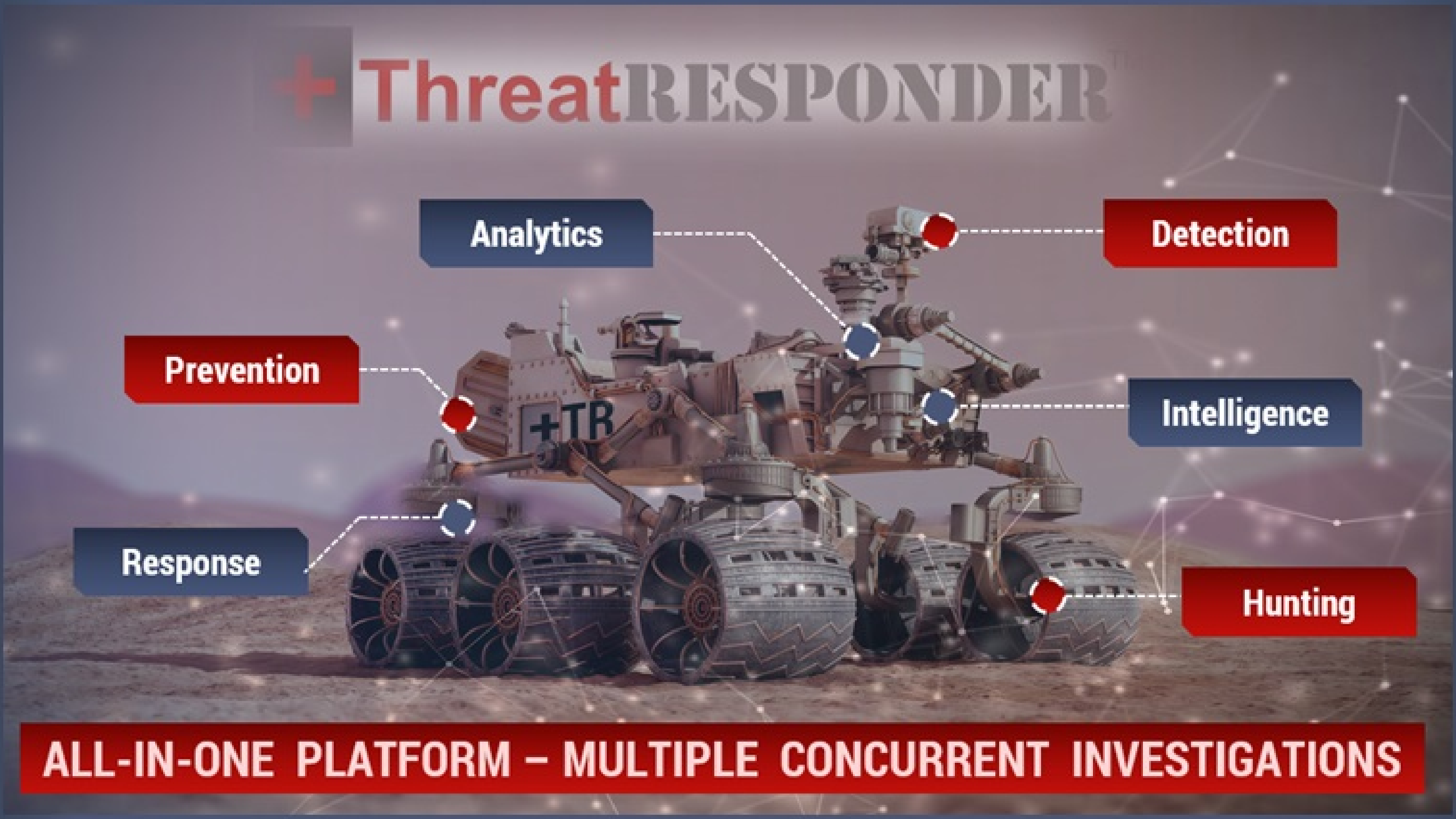
Red Hat Security Advisory 2023-3366-01 - Red Hat OpenShift Container Platform is Red Hat's cloud computing Kubernetes application platform solution designed for on-premise or private cloud deployments. This advisory contains the RPM packages for Red Hat OpenShift Container Platform 4.13.2. Issues addressed include a traversal vulnerability.

## Are You…

- Spending several hours, days, or weeks conducting forensic investigations?
- Using different and unnecessary tools that pose correlation challenges?
- Wasting money on needless travels?
- Overworked, understaffed, and facing a backlog of cases?
- Uploading potentially sensitive files to VirusTotal or third-party sites?

## Do DFIR Investigations Better

- Conduct DFIR investigations on any remote endpoint regardless of its geolocation – all on a single-pane of glass
- Perform in-depth forensics investigation dating back to the first day the target endpoint was installed
- Conduct full dynamic and static malware analyses with just a click of a mouse
- Conduct legally-defensible multiple DFIR cases simultaneously



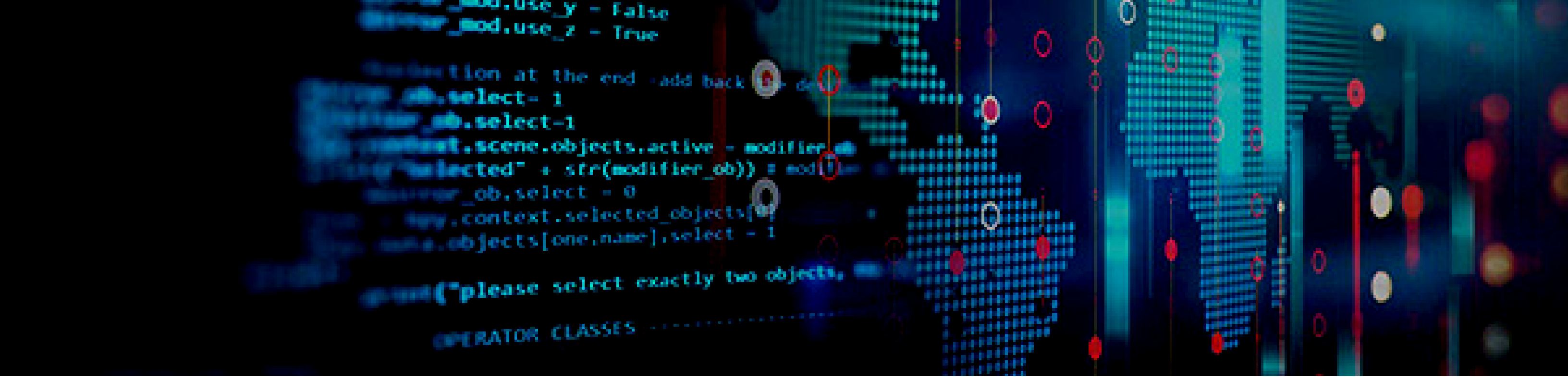
## The Solution – ThreatResponder® Platform

**ThreatResponder® Platform** is an all-in-one cloud-native endpoint threat **detection**, **prevention**, **response**, **analytics**, **intelligence**, **investigation**, and **hunting** product

## Get a Trial Copy

Mention **CODE: CIR-0119**

**https://netsecurity.com**



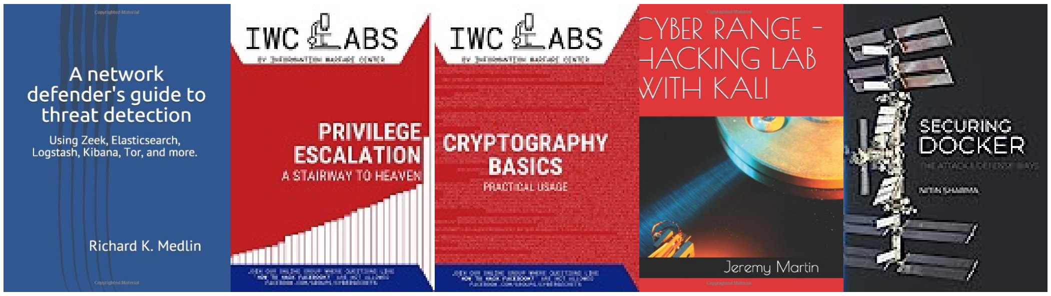
# The Cyber Secrets publications on Amazon

The Cyber Weekl Awareness Report (WAR) is an Open Source Intelligence (AKA OSINT) resource centering around an array of subjects ranging from Exploits, Advanced Persistent Threat, National Infrastructure, Dark Web, Digital Forensics & Incident Response (DIFR), and the gambit of digital dangers.

Items that focus on cyber defense and DFIR usually spotlight capabilities in the CSI Linux environment.  If interested in helping evolve, please let us know.  The Cyber Secrets publications rotates between odd quarters issues focusing on Blue Team and the even issues on Red Team.

CYBER Secrets
Information Warfare Center
What's Inside?
Visit our YouTube Channel
Threat Intelligence & Training
CYBER SECRETS
DIVE INTO THE 5TH DOMAIN THREAT INTELLIGENCE
RED TEAMING AROUND YOUR BACKYARD
WHILE DRINKING OUR JUICE IN THE HOOD
THE 8 LAYERS OF THE OSI CAKE
A FORENSIC TASTE OF EACH LAYER
LAUNCHING EXPLOITS
ONE SMALL VULNERABILITY FOR A COMPANY, ONE GIANT HEAP FOR PORT BIND.
INCIDENT RESPONSE DO NOT CROSS
INCIDENT RESPONSE
EVIDENCE PRESERVATION AND COLLECTION
JOIN OUR ONLINE GROUP WHERE QUESTIONS LIKE "HOW TO HACK FACEBOOK?" ARE NOT ALLOWED
FACEBOOK.COM/GROUPS/CYBERSECRETS

# Other Publications from Information Warfare Center


A network defender's guide to threat detection
Using Zeek, Elasticsearch, Logstash, Kibana, Tor, and more.
Richard K. Medlin
IWC LABS
PRIVILEGE ESCALATION
A STAIRWAY TO HEAVEN
IWC LABS
CRYPTOGRAPHY BASICS
PRACTICAL USAGE
CYBER RANGE - HACKING LAB WITH KALI
Jeremy Martin
SECURING DOCKER
THE ATTACK & DEFENSE WAYS
NITIN SHARMA

# CYBER WEEKLY AWARENESS REPORT

VISIT US AT **INFORMATIONWARFARECENTER.COM**

THE IWC ACADEMY
**ACADEMY.INFORMATIONWARFARECENTER.COM**

FACEBOOK GROUP
**FACEBOOK.COM/GROUPS/CYBERSECRETS**

CSI LINUX
**CSILINUX.COM**

CYBERSECURITY TV
**CYBERSEC.TV**

ARGOS APPLIED INTELLIGENCE

INFORMATION WARFARE CENTER

CSi LINUX

netSecurity®

ThreatRESPONDER

Accredited Training Center EC-Council

CYBERQ GROUP